Medeco Security Locks Guide



Developing and Managing Key Control Policies and Procedures

medeco®
HIGH SECURITY LOCKS

Table of Contents

Authors:

Lee A. Garver, DAHC
Corbin Russwin Architectural Hardware
Berlin, CT

Clyde T. Roberson, CML, AHC, CPP
Medeco Security Locks
Salem, VA

David A. Steele
Sargent Manufacturing Company
New Haven, CT

Original Publication: June 2005

I. Introduction

This manual is brought to you by ASSA ABLOY, the world's leading group of manufacturers and suppliers of locking solutions, dedicated to satisfying end-users' needs for security, safety, and convenience. It represents hundreds of years of best practices developed and observed by providing the world's finest key systems.

This manual recognizes that providing key systems and associated hardware is only the beginning. For our customers to successfully enjoy the benefits of the products we furnish, and to extend the life and value of a key system, a proper key management system must be in place. The policies and procedures suggested in this manual can play an essential part in increasing the safety and security of any facility.

This manual should be used as a model or guide only. End users are encouraged to adopt all or part of the recommendations as appropriate to meet their individual needs.

Disclaimer: ASSA ABLOY encourages the use in whole or part of this document but does not imply or warrant fitness for any purpose other than for reference only. Its use in whole or part is solely the decision and responsibility of the adopting facility.

II. Comprehensive Key Control Policy

A. Purpose

1. The purpose of this Key Management Policy is to help protect the life, property, and security of this facility and all its occupants.

2. It shall serve as the framework by which all keys and access credentials will be managed, issued, duplicated, stored, controlled, returned, replaced, and accounted for by the Key Control Authority ("KCA").

    2.1. The KCA comprises the person, persons, department, or committee that has authority to adopt, administer, and enforce this facility's Key Management Policy.

    2.2. This policy shall apply to all keys including those to all space, office equipment, vehicles, padlocks, lockers, safes, etc. owned, operated, or controlled by the facility.

3. This Policy seeks to establish a recorded chain of accountability and access for all credentials, keyholders, and locations.

    3.1. Establish a key issuance authority.

    3.2. Issue appropriate level keys to individuals.

    3.3. Establish authority on all key control policies.

4. This policy seeks to implement a proper key control process and then preserve it by restoring security in a timely manner whenever key control has been threatened or compromised.

B. Specification

1. This facility shall use a key control system and adopt administrative policies that facilitate the enforcement of Key Management Procedures as outlined in this *Guide to Developing and Managing Key Control Policies and Procedures.*

2. The following represent the basic and most critical elements of key control and shall be included, as a minimum, in the key control specification.

    2.1. Facility shall appoint a Key Control Authority and/or Key Control Manager to implement, execute, and enforce key control policies and procedures.

    2.2. A policy and method for the issuing and collecting of all keys shall be implemented.

    2.3. Keys and key blanks shall be stored in a locked cabinet or container, in a secured area.

    2.4. A key control management program shall be utilized. A dedicated computer software application is preferred—Key Wizard® or equivalent.

    2.5. All keys shall remain the property of the issuing facility.

    2.6. A key should be issued only to individuals who have a legitimate and official requirement for the key.

        2.6.1. A requirement for access alone, when access can be accomplished by other means (such as unlocked doors, request for entry, intercoms, timers, etc.), shall not convey automatic entitlement to a key.

    2.7. All keys shall be returned and accounted for.

    2.8. Employees must ensure that keys are safeguarded and properly used.

C. Enforcement

1. This policy shall be adopted by universal consent and administrative mandate from the highest levels to allow full and complete implementation and enforcement.
2. All keys remain the property of facility.
3. Keys that are no longer required for authorized purposes shall be returned to the Key Control Authority (KCA).
4. No person or department shall knowingly receive, borrow, or possess any key for any space without receiving permission from a person duly authorized to give permission to possess such key.
5. No person shall knowingly alter, duplicate, copy, or make a facsimile of any key to a lock of a facility building or property without receiving permission from the KCA.
6. To enforce effective key control, administrators may choose to impose a deposit for each key issued.
7. Keyholders shall use assigned keys for access to authorized locks only.
8. Keyholders shall take measures to protect and safeguard any facility keys issued to them or in their name.
9. Keyholders shall not loan their facility key(s).
10. Keyholders shall not use their key(s) to grant access to non-authorized individuals.
11. Keyholders shall not attempt in any manner to duplicate or alter facility keys in their possession.
12. Keyholders shall immediately report any lost, missing, stolen or damaged keys.
13. Persons entering locked buildings or spaces are responsible for re-securing all doors and shall not prop open any doors.
14. Individuals shall not store keys in desk drawers or other unsecured areas.
15. Violations of any of these enforcement policies may result in disciplinary action up to and including dismissal.

D. Elements of a Key Control Policy

Key Control Authority—"KCA"

1. Facility shall appoint a Key Control Authority with power and authority to:
   - 1.1. Develop all the policies and procedures related to the facility's key management system.
   - 1.2. Appoint or become a Key Control Manager to:
     - 1.2.1. Implement, execute and enforce the key control policies and procedures.
     - 1.2.2. Issue and return keys with proper documentation, authorization, and transaction receipts.
     - 1.2.3. Supervise, authorize, and control the security of key and key blank storage and the key cutting process.

Storage

1. Keys, credentials, and key records shall be stored in a secure condition (data) or location (physical items) protected by lock and key or vault.
   - 1.1. Keys shall be stored in a locked cabinet or container, in a secured area.
   - 1.2. Key rings issued for temporary use shall be of a tamper resistant design so that keys cannot be removed from the ring prior to return.
   - 1.3. Keys stored in a non-centralized location:
     - 1.3.1. Sequence locks release one key upon the insertion and trapping of another.
       - 1.3.1.1. Allows remote issuance of master keys.
       - 1.3.1.2. Permits fewer master keys to be issued on a permanent basis.
     - 1.3.2. Emergency key storage boxes (Knox, Supra type).
       - 1.3.2.1. Subject to local regulations and to protect against theft or duplication, no master keys should be stored in these types of containers.
     - 1.3.3. Computerized key cabinets with access control and audit capability may be used in remote locations for temporary key issuance.
   - 1.4. Key records shall be stored in a secure location that is protected against both fire and theft:
     - 1.4.1. Bitting lists.
     - 1.4.2. Authorization forms.
     - 1.4.3. Key issuance and return records.
     - 1.4.4. Data files shall be password protected and encrypted.

Key Management Formats

The key management system shall be maintained in either a manual or computerized format.

1. The manual format shall use card and index files to easily access, maintain, and cross-reference information on:

 1.1. Keys:

  1.1.1. Blind code numbers.

  1.1.2. Standard Key Coding Symbols ("SKCS").

  1.1.3. Key identity: serial, inventory, or sequence number.

  1.1.4. Individuals with authority to issue for each key.

  1.1.5. Temporary issue keys and key rings.

 1.2. Keyholders:

  1.2.1. Name, address, ID #, telephone, key deposit.

  1.2.2. Authorized individual's signature.

  1.2.3. Optionally: signature, photo, PIN.

  1.2.4. Key deposit (if any).

 1.3. Locations:

  1.3.1. Room number.

  1.3.2. Door number.

  1.3.3. Description or usage.

  1.3.4. Departmental control.

  1.3.5. Security level or access restrictions.

 1.4. Hardware:

  1.4.1. Lockset, exit devices, deadbolt.

  1.4.2. Cylinder type.

  1.4.3. Door closer.

  1.4.4. Hinges.

  1.4.5. Finish.

  1.4.6. Protection plates.

2. The computerized format shall use password protected and data encrypted software to easily access, maintain, and cross-reference information on:

   2.1. Keys:
   - 2.1.1. Blind code numbers.
   - 2.1.2. Standard Key Coding Symbols ("SKCS").
   - 2.1.3. Key identity: serial, inventory, or sequence number.
   - 2.1.4. Individuals with authority to issue for each key.
   - 2.1.5. Temporary issue keys and key rings.

   2.2. Keyholders:
   - 2.2.1. Name, address, ID #, telephone, key deposit.
   - 2.2.2. Authorized individual's signature.
   - 2.2.3. optionally: signature, photo, PIN.
   - 2.2.4. Key deposit (if any).

   2.3. Locations:
   - 2.3.1. Room number.
   - 2.3.2. Door number.
   - 2.3.3. Description or usage.
   - 2.3.4. Departmental control.
   - 2.3.5. Security level or access restrictions.

   2.4. Hardware:
   - 2.4.1. Lockset, exit devices, deadbolt.
   - 2.4.2. Cylinder type.
   - 2.4.3. Door closer.
   - 2.4.4. Hinges.
   - 2.4.5. Finish.
   - 2.4.6. Protection plates.

3. Either format used shall allow a fully searchable cross-reference:
   - 3.1. Keys x location(s).
   - 3.2. Keys x keyholder(s).
   - 3.3. Keyholder x keys.
   - 3.4. Keyholder x location(s).
   - 3.5. Location x key(s).
   - 3.6. Location x keyholder(s).

Record Keeping

1. All key records shall be kept current at all times and are to be considered high security and confidential.
2. Records shall be securely stored (see “Storage”).
3. All transactions shall be recorded in a timely manner.
4. Standardized forms shall be used (see “Forms”).

Policies and Procedures

1. Identifying Keys and Keying

1.1. All keys should only be marked with a blind code number that does not in any way reflect its usage or level.

1.2. The use of standard key coding to mark cylinders or keys is not recommended.

1.3. Keys should not be marked M, MK, GMK, or GGMK to indicate level of keying.

1.4. All issued keys should contain an inventory or serial number that reflects the total number of keys issued and provides a unique identifier for every copy.

1.5. Keys should not be stamped with bittings.

2. Issuing Keys

2.1. All key orders should be properly authorized by an authorized signer, in addition to the keyholder, before issuing.

- 2.1.1. Each key can have its own appropriate level of authorization.
  - 2.1.1.1. Higher level keys may require higher levels of authorization.

2.2. Issue the proper level key to each individual granting only the appropriate level of access.

2.3. Issue keys by need, not desire.

2.4. Require signature(s) on keyholder agreement:

- 2.4.1. Signature of keyholder.
- 2.4.2. Signature of authorizer.

2.5. Require photo ID.

2.6. Keys shall be issued by duration of need, not by term of employment.

2.7. Signature required by keyholder and authorizer.

2.8. Keys must be personally picked up, not mailed.

- 2.8.1. If necessary, keys may be delivered by courier or other return-receipt-required certified carrier.

2.9. Keys shall be individually serialized or numbered.

 2.9.1. Keys shall be identified by blind code numbers and serialized number.

2.10. Individuals may be issued only one copy of each keyset.

 2.10.1. Exception for approved multiple key holders.

2.11. The KCA shall establish key issuance authorization levels determined by the type of key. The general rule shall be that an authorizer may only approve keys for spaces directly under his/her control. In some cases more than one authorizer may be required.

 2.11.1. Types of keys:

  2.11.1.1. Change keys.

  2.11.1.2. Master keys.

  2.11.1.3. Grand master keys.

  2.11.1.4. Top master key.

  2.11.1.5. Entrance key.

  2.11.1.6. Control keys.

  2.11.1.7. Mechanical/Maintenance keys.

  2.11.1.8. SKD/Security keys.

2.12. Facility shall use standardized key deposits varying by keyholder type and by level of key. For example, the deposit for a master key should be greater than that of a change key.

2.13. Keys may not be duplicated or issued except through the KCA or authorized facility locksmith.

2.14. Keys shall only be issued by a designated individual.

 2.14.1. Exception: electronic key cabinets with audit control or sequence locks.

2.15. All keys should be tracked with a return due date and time, especially temporary issue keys.

2.16. Shift keys or rings shall be returned at the end of every work shift.

2.17. Shift key rings shall be sealed and tamper evident.

3. Returning Keys

3.1. All keys shall be returned to the issuing department by the authorized keyholder.

 3.1.1. When keys are returned, any key deposit will be refunded and a key return receipt shall be issued to the keyholder.

3.2. Found keys must be turned into the KCA.

3.3. Final paychecks, records, and/or transcripts may be held pending return of key(s).

4. Non-returned key policy

4.1. A fee for lost or stolen keys shall be established.

4.1.1. In the event that facility keys are lost or stolen, it shall be policy to recombinate immediately any cylinders accessible by the lost key(s).

4.1.2. All re-keying charges must be paid by department, individual, or company responsible for losing the key.

4.1.3. Rekeying charges shall be determined by the number of locks operated by the lost or stolen key(s).

4.1.4. If any individual has two or more separate incidents of lost, stolen, or non-returned key violations within a one-year period, key privileges may be revoked.

5. Administration of the Master Key System

5.1. Update the key schedule and bitting lists as new codes and bittings are issued and used.

5.1.1. Send periodic updates to the cylinder manufacturer if factory control over the key system will continue.

5.2. Cross keyed conditions should be minimized or avoided.

5.2.1. When cross keying is unavoidable, all cross keyed conditions should be fully recorded.

6. Audits

6.1. Keyholder:

6.1.1. On at least an annual basis, the responsible department will determine that the proper accountability of keys is being maintained by conducting random key checks that sample the keys being carried by at least 25% of all departmental keyholders.

6.2. Key System:

6.2.1. It is recommended that, under normal circumstances, all keys and cylinders should be changed, or at least evaluated for change, at intervals not exceeding five years.

6.2.2. Perform periodic audits of key cutters to determine if unauthorized duplicate keys can be obtained.

6.3. Reports shall be periodically generated and distributed by department with a written response required to confirm the accuracy of the information being held.

7. Transfer/Temporary use

7.1. Keys shall not be transferred from one individual to another without proper authorization and record keeping from the KCA.

Forms

It is highly recommended that forms be developed to document all key transactions.

The following represents basic elements that should be included in one or more of each type of form — *see example next page.*

1. **Key Request Form**
    - 1.1. Key request:
        - 1.1.1. One form for one key.
        - 1.1.2. Issue multiple forms for multiple keys.
    - 1.2. Key issue agreement.
    - 1.3. Keyholder signature.
    - 1.4. Authorization signature.
    - 1.5. Work order.
    - 1.6. Key issue and deposit receipt.
    - 1.7. Multiple keyholder request.

2. **Key Return Form**
    - 2.1. Key return receipt.
    - 2.2. Deposit return receipt.

3. **Lost or Stolen Key Report Form**
    - 3.1. Description of circumstances of loss.
    - 3.2. Rekey fee if any.

4. **Service Form**
    - 4.1. Cylinder recombination form.
    - 4.2. Request for SKD or NMK keying.
    - 4.3. Lock opening request form.

The following basic information should be included on each form.

1. Key holder name, address, ID and/or department.
2. Signature of key holder and date.
3. Key identification (key set symbol and/or blind code).
4. Location where key(s) are needed.
5. Type of transaction; issue, return, lost or stolen, cylinder recombination, or lock opening request.
6. Authorization signature(s).
7. Date of specific transaction(s).

Key Request Form

(Use one form for each key only)

Name ____________________

Employee ID# ____________________ Phone ____________________

Key# ____________ Key Symbol ________ Copy# ______ Mfgr ____________

Key Location(s) ____________________

____

Key Issue Agreement: In return for the loan of this key, I agree: **1)** not to give or loan the key to others; **2)** not to make any attempts to copy, alter, duplicate, or reproduce the key; **3)** to use the key for authorized purposes only; **4)** to safeguard and store the key securely; **5)** to immediately report any lost or stolen keys; **6)** produce or surrender the key upon official request. I also agree that if the key is lost, stolen, or not surrendered when requested a charge that reflects the cost of changing any and all locks affected may be assessed.

Signature ____________________ Date ____________

Deposit ____________

Issue Type:
- ❑ Standard
- ❑ Temporary   Due Date ____________
- ❑ Reissue   Reason ____________

Authorizer's Signature ____________________ Date ____________

Print Name ____________________

Title ____________________

Phone ____________________

OFFICIAL USE ONLY

DATE ISSUED ____________________

BY ____________________

CONTROL # ____________________

ENTERED BY ____________________

KEY RETURN:

RETURN DATE ____________ **BY** ________

RETURN REASON ____________________

____

DEPOSIT RETURN ____________________

KEY NOT RETURNED:
❑ LOST ❑ STOLEN ❑ BROKEN ❑ OTHER

EXPLAIN CIRCUMSTANCES: ____________

____

____

SIGNATURE RECEIPT ____________

BY ____________________

Servicing

1. **Cutting keys:**
   1.1. Only a facility-approved locksmith shall be permitted to cut keys.
   1.2. All facility keys shall be cut on factory approved code cutting machines, not on duplicating machines that trace from one key to another. Duplicating machines are less accurate and can transfer wear or inaccuracy that worsens through generations of keys.

2. **Pinning/recombinating cylinders:**
   2.1. Shall only be performed by facility-approved locksmith department.
   2.2. Shall be on the facility's key system unless approved by KCA.
      2.2.1. Combinate to all appropriate levels of keying unless pre-approved by KCA.
      2.2.2. SKD combinations must be pre-approved by KCA.

3. **Installing locks:**
   3.1. Shall only be performed by facility-approved locksmith department.
   3.2. Shall be on facility's key system unless approved by KCA.

4. **Preventative maintenance shall be performed regularly to ensure proper operation of keys and locks and to maintain security.**
   4.1. Worn keys shall be replaced to avoid breakage.
   4.2. Worn or poorly functioning cylinders shall be replaced to maintain proper security.
   4.3. All facility key machines shall be checked and calibrated regularly, at least on a monthly basis.

5. **Locksmithing work shall only be performed by:**
   5.1. An in-house locksmith department, or
   5.2. A facility-approved outside locksmith business.

III. Condensed Model Key Control Policy

The following is to be used as a guide for developing a key control policy, and to assist in the understanding of how a formalized key control policy should be formatted. When used in conjunction with the Key Control Policy Elements of Medeco Security Locks' Guide to Developing and Managing Key Control Policies and Procedures, this sample key control policy can be tailored to meet a facility's specific key management objectives.

Purpose

The purpose of this Key Control Policy is to help protect the life, property, and security of this facility and all its occupants.

Specification

This facility shall use a key control system and administrative policies that facilitate the adoption and enforcement of this Key Control Policy.

General

The introduction of a key control policy is essential for the security of this facility and the protection of personnel, property, and equipment.

Facility shall appoint a Key Control Authority with power and authority to: develop all policies and procedures related to the facility's key management system; and, appoint or become the Key Control Manager to execute and enforce key control policies and procedures.

The Locksmith Shop (internal or contracted service), unless otherwise directed, is responsible for making keys, installing and maintaining locks and cylinders.

No person shall knowingly alter, duplicate, copy, or make a facsimile of any key to a lock of a building or property thereof without receiving permission from a person duly authorized.

Key Control

The Key Control Authority will determine appropriate policy and method for the issuing and collecting of all keys.

All keys shall be stored in a secured locked cabinet.

The Key Control Authority shall utilize an effective key control management program and assign the appropriate individual(s) to maintain its use.

To facilitate effective key control, the Key Control Authority may impose a nominal key deposit.

Policy and Procedures

Issuing of Keys
All keys remain the property of _____________(Insert name of facility).

All keys shall be properly authorized by signature before issuing, and shall only be issued by a designated individual.

The process for which keys shall be issued will be based on defined policies and procedure as set forth by the Key Control Authority.

Keys should be issued only to individuals who have a legitimate need for the key.

The number of master keys issued should be limited.

Returning Keys
All keys shall be returned to the issuing department by the keyholder of record.

All lost keys shall be reported immediately to the Key Control Authority. It shall be the facility's policy that when keys are lost or stolen, to recombinate immediately any cylinders accessed by the lost keys.

All found keys shall be returned to the Key Control Authority.

Employee Responsibilities
Employees shall only use their keys to access their assigned work areas and should lock doors when leaving any secured area. Employees must also ensure that keys are safeguarded and properly used.

The unauthorized possession, use or reproduction of a key may constitute theft or misappropriation. Any employee who violates this policy may be subject to disciplinary action.

IV. Specific Applications

1. Educational, K-12
2. Healthcare Facilities
3. Colleges and Universities
4. Office Buildings

Educational K-12

Following are specific examples of additional elements that should be considered when tailoring a key control policy for Educational, K-12 facilities:

1. K-12 facilities require heightened lock and key management to protect a highly vulnerable population of students and staff.
    - 1.1. Any policy must restrict the distribution and ensure the retrieval of keys.
    - 1.2. Access through entrance doors must be tightly controlled.
    - 1.3. Threats: drugs, kidnappings, vandalism, terrorism, violence, abuse.
2. Lockdown conditions and procedures.
3. Limited school year with extended periods of vacation or closure that require return of keys or lock-out of many keyholders.
4. Community usage and access requirements:
    - 4.1. Special access authorization requirements.
    - 4.2. Special requirements for unlocking requests.
5. A school district may have many buildings, often spread over a wide geographical area.
    - 5.1. This may require special considerations for service, remote key duplication and issuance.
6. Unique types of keyholders:
    - 6.1. Teachers.
        - 6.1.1. Keys should normally be returned at end of academic year.
    - 6.2. Substitute teachers.
        - 6.2.1. Temporary issued keys.
    - 6.3. Administration.
    - 6.4. Maintenance/Service/Security.
7. Administered by local government and subject to state, federal, and local laws.

Healthcare Facilities

Following are specific examples of additional elements that should be considered when tailoring a key control policy for Healthcare facilities.

Healthcare facilities, including hospitals, clinics, and nursing homes provide unique demands upon a key system. Facilities protecting a more vulnerable population, such as children, the sick or infirm, the aged, those with infectious diseases, those susceptible to infection, or those with mental impairment, even including the criminally insane, can present a diverse set of needs. Some of those considerations are:

1. Healthcare facilities ("HCF's") may require a strong KCA that can enforce key issuance and return policies despite the strong needs and powerful personalities of doctors and administrators.

2. HIPPA privacy requirements.

3. HCF's have different departments with varying security needs:
   - 3.1. Obstetrics.
   - 3.2. Pediatric wards.
   - 3.3. Psychiatric detention areas.
   - 3.4. Infectious disease areas.
   - 3.5. Emergency rooms.
   - 3.6. Elderly care with anti-wandering requirements.
   - 3.7. Unique elevator controls.
   - 3.8. Pharmacy: storage and dispensary.
   - 3.9. Security department with full access abilities.
   - 3.10. Custodial and cleaning staff must have full access to keep high sanitation standards.
   - 3.11. Radiology.
   - 3.12. Laboratories.

4. HCF's often allow free access, 24x7x365, to visitors and attendants, but still require a high degree of control within the building itself.

5. An HCF may have many buildings united under one key system.

6. Unique types of Keyholders:
   - 6.1. Doctors.
   - 6.2. Nurses.
   - 6.3. Administrators.
   - 6.4. Maintenance and technicians.
   - 6.5. Cleaning supervisors.
   - 6.6. Security.
   - 6.7. Temporary staff with high turnover.
   - 6.8. Outside contractors.
   - 6.9. Researchers.
7. Unique accreditation and federal, state and local government inspection and legal requirements.

Colleges and Universities

Following are specific examples of additional elements that should be considered when tailoring a key control policy for colleges and universities.

1. Colleges and universities require heightened security measures in lock and key management to protect a highly vulnerable population of faculty, staff and students.
    - 1.1. Any policy must restrict the distribution and ensure the retrieval of keys.
    - 1.2. The key control policy must properly blend the needs of the physical security locking system with other access control measures.
    - 1.3. Different security needs for academic buildings, housing—undergraduate and graduate, on-campus and off-campus—administrative, physical plant, and other outside contracted services must also be considered in the key control policy.
    - 1.4. Threats: theft, vandalism, terrorism, violence, student pranks, protesters.

2. Colleges and universities may have many different department types and usages with varying requirements. They may include:
    - 2.1. Academic.
    - 2.2. Dormitories and Commons (or simply Housing).
    - 2.3. Athletics.
    - 2.4. Real Estate.
    - 2.5. Apartments.
    - 2.6. Hotels and lodging.
    - 2.7. Physical Plant.
    - 2.8. Government and industry research laboratories.

3. Standard school year calendar with extended breaks or closure that require return of keys or lock-out of keyholders.

4. Community usage and access requirements:
    - 4.1. Special access authorization requirements.
    - 4.2. Special requirements for unlocking requests.

5. Types of Keyholders:
    - 5.1. Administrators.
    - 5.2. Staff.
    - 5.3. Professors.
    - 5.4. Maintenance and security.
    - 5.5. Students.
        - 5.5.1. Keys should normally be returned at end of academic year, or during periods of lock out.
    - 5.6. Contracted services.
        - 5.6.1. Temporary issued keys, to be returned as specified
    - 5.7. Researchers.

Office Buildings

The following are examples of additional elements that should be considered when tailoring a key control policy for Office Buildings.

1. Administration of tenant space v. core space.
   - 1.1. Tenant space belongs to the office and retail occupants of a building and can change regularly both in size, structure and composition.
   - 1.2. Core space is the backbone or support area of a building represented by private mechanical, electrical, communications, janitorial, roof as well as public areas such as stairwells, lobbies, shipping and loading areas, parking areas, etc.

2. Tenants often request or insist upon their own key system and key management procedures managed independently from building management.
   - 2.1. Each tenant may have its own KCA or should use one provided by building management.

3. Administration and structure of keys and key system are often designed by floor and may or may not overlap with the structure of tenant usage.

4. High traffic flow of public non-keyholders during the day (though more and more may be required to be escorted or identified first), versus very limited access after hours.

5. Vacant or unoccupied space.

6. High rate of change and redesign of the key system with tenant turnover.

V. Glossary of Terms and Definitions

This glossary of terms and definitions relates to this Key Control Policy and should not be considered universal.

For a complete listing of all terms relating to cylinders, keys and master keying references refer to ALOA's sponsored publication *The Professional Glossary of Terms Relating To Cylinders, Keys, and Master Keying.*

Any definitions herein that were adopted from ALOA's publication are indicated by an asterisk.

Bitting*
1. The number(s) which represent(s) the dimensions of the key cut(s).
2. The actual cut(s) or combination of a key.

Blind Code Number*
A designation, unrelated to the bitting, assigned to a particular key combination for future reference when additional keys or cylinder may be needed.

Change Key
Change Key (CK) – sometimes referred to as "Day Key."
The lowest level key in a key system.

Credential
See key

Controlled Cross Keying *
A condition in which two or more different keys of the same level under the same higher level key(s) operate one cylinder by design, i.e. XAA1 operated by AA2 code symbol.

Cross Keying
The deliberate process of combinating a cylinder (usually in a master key system) to two different keys which would not normally be expected to operate it together.

Pinning a cylinder in a key system to additional keys other than those identified to operate the cylinder based on the cylinder's Standard Key Code key symbol.

Control Key
A key to remove and/or install an interchangeable or removable core.

Grand Master (GM)
The TMK in a 3 level Master Key system, or a Grand Master (GM) key in a higher level Master Key system.

Great Grand Master (GGM)

The TMK in a 4 level Master Key system, or a Great Grand Master (GGM) key in higher level Master Key system.

Great Great Grand Master (GGGM)

The TMK in a 5 level Master Key system or a Great Grand Master (GGM) key in a higher level Master system.

Key

A token, credential, or device used to grant or deny access. For this manual the word "key" shall refer to electronic and mechanical devices.

Key Control*

Any method or procedure which limits unauthorized acquisition of a key and/or controls distribution of authorized keys. A systematic organization of keys and key records.

Key Control Authority (KCA)

The individual or group having responsibility and jurisdiction for creating, enforcing, and administering all key control policies and procedures.

Key Symbol*

A designation used for a key combination in the standard key coding system, e.g., A, AA, AA1, etc.

Keyed Alike (KA)*

Of or pertaining to two or more locks or cylinders which have or are to have the same combination. They may or may not be part of a keying system.

Keyway (Kwy)

A pattern of milling (warding) groove configurations of that appear on each side of the key blank that may be for a single keyway or a family of key sections that are part of a multiplex keyway family.

Key Section

A single grooved pattern that is milled onto each side of a key blank and is one of a series of groove patterns belonging to the same factory keyway family.

Master – Key Sections

A grove pattern representing different individual key sections that are milled into each side of a single key blank. These milling patterns are part of a pre-defined group of groove patterns all belonging to the same factory keyway family.

Master Key (MK)

The TMK in a level 2 Master Key system, or Master Key (MK) in a higher level Master Key system.

Multiple Keyholder

An individual authorized to be issued multiples of any single key for purposes of bulk key issue.

Multiplex Key Blank

A key blank whose side milling or wardings are part of a manufacturer's particular series of key sections.

Multiplex Master Key System

A master key system that takes advantage of a manufacturer's sectional keyway family to create very large master key systems.

NMK - Not Master Keyed

Used as a suffix to a key set that indicates the cylinder built to this key symbol is only to be operated by the change key and no master level keys are to operate the in the cylinder. This term maybe interpreted differently by various manufacturers. NMK may mean that only the Master Key is not to operate in the cylinder. You may also see NGMK meaning only the GM key is not to operate in the cylinder, or NGGMK meaning that only the GGMK key is not to operate in the cylinder.

Sequence Lock

A lock designed to retain one or more keys captive until another key is inserted, turned and trapped. The second key is retained until the first key is returned and turned to the captive position.

Shift Keys

Keys or key rings issued to individuals only for the duration of their work period, to be returned at the end of his/her work shift.

TMK * - Top Master Key

The highest level master key in a particular key system.

Uncontrolled Cross Keying*

A condition in which two or more different keys under different higher level key(s) operate one cylinder by design, i.e. XAA1 Operated by AB1

VKC - Visual Key Control System

The stamping of cylinders and/or key bows in a master key system with the "Standard Key Coding System" identification symbol.

UL437

The Underwriters Laboratory Test Standard for High Security Cylinders.

Some of these terms and definitions have been taken from *The Professional Glossary of Terms Relating to Cylinders, Keys, and Master Keying*, developed by the "Master Keying Study Group of the ALOA Sponsored Task Group for Certified Training Programs."

The Professional Glossary of Terms Relating to Cylinders, Keys, and Master Keying is a recognized standard in the hardware industry for terms and definitions related to cylinders and keys used by the manufacturers and users of products generated by the hardware locking industry.

Any terms and definitions taken from the *The Professional Glossary of Terms Relating to Cylinders, Keys, and Master Keying* that appear in this document are marked with an (*) asterisk. Any terms not marked with the asterisk are terms and definitions that have evolved over the years at ASSA ABLOY AMERICA and continue to be applied in the everyday processing of cylinders, keys and master keying systems.
Non- asterisked terms appearing in this book should not be construed as being necessarily recognized as the standard by all manufacturers.

medeco
HIGH SECURITY LOCKS

Medeco US: 3625 Allegheny Drive • Salem, Virginia 24153
Customer Service 1.800.839.3157

Medeco Canada: 141 Dearborn Place • Waterloo, Ontario N2J 4N5
Customer Service 1.888.633.3264

www.medeco.com

Founded in 1968, Medeco is a market leader in manufacturing high security, patent protected locks and locking systems for security, safety, and key control. The company's customer base includes Wholesale and Retail Security providers, Original Equipment Manufacturers, and Industrial End-users.

The ASSA ABLOY Group is the world's leading manufacturer and supplier of locks and associated products, dedicated to satisfying end-user needs for security, safety, and convenience.

ASSA ABLOY

LT-922093 REV A